The Group Diffie-Hellman Problems

Emmanuel Bresson
(ENS, France)

Olivier Chevassut (LBNL, USA)

David Pointcheval (ENS, France)

OUTLINE

- Motivation
- Related Work
- Two-party Diffie-Hellman key exchange
- Group Diffie-Hellman key exchange
- Relation between the group DH problems and the DH problems
- Conclusion

Motivation

- An increasing number of distributed applications need to communicate within groups, e.g.
  - collaboration and videoconferencing tools
  - replicated servers and distributed computations
- An increasing number of applications have security requirements
  - privacy of data
  - protection from hackers, viruses and trojan horses
- A method to establish a group session key is needed

Objectives

- Studying algorithmic problems in the discrete logarithm setting
  - Diffie-Hellman problems
  - Group Diffie-Hellman problems
- Why finding reductions between the group DH and the two-party DH problems
  - To get confindence in the group DH problems
  - To correctly chooose security parameters for them
  - To securely design group key agreement protocols

Related Work

- Design methodology
  - based on complexity theory
  - successful at avoiding flaws
  - useful to validate cryptographic algorithms

- Prior Results
  - « Group DH key exchange under standard assumptions », Eurocrypt ’02
  - « Provably authenticated group DH key exchange - dynamic case », Asiacrypt ’01
  - « Provably authenticated group DH key exchange », ACM CCS ’01

Provable Security Methodology

1. Specification of a model of computation

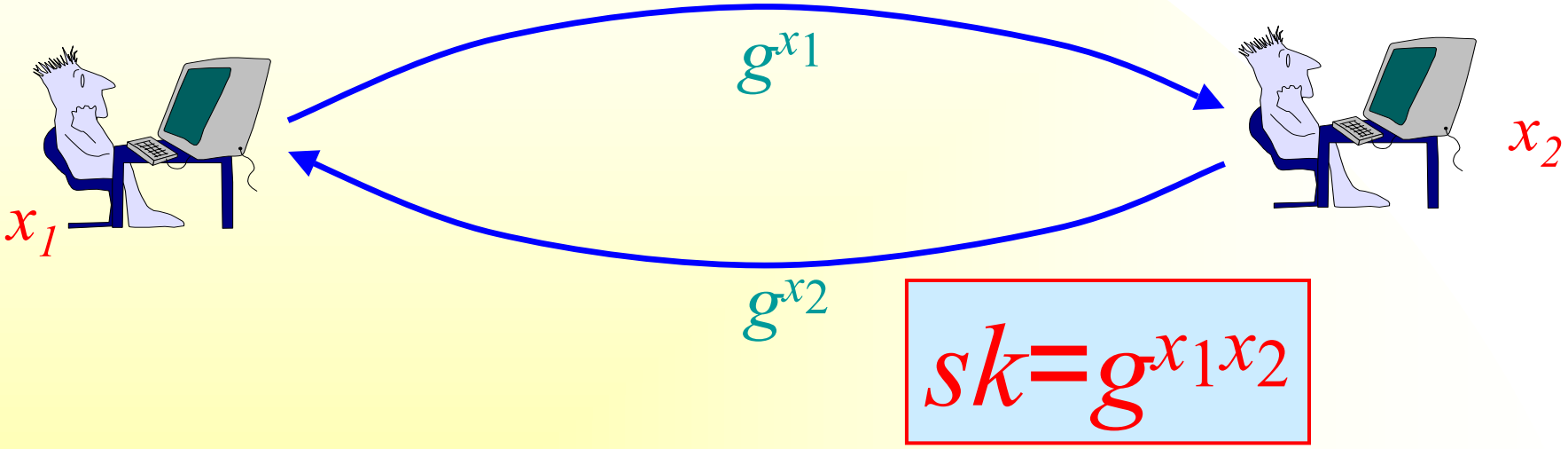
2. Definition of the security goals

3. Statement of the intractability assumptions
   - computational/decisonal Diffie-Hellman problems (CDH/DDH)
   - group computational/decisional DH problems (GCDH/DDH)

4. Description of a group DH key exchange scheme and its proof of security
   - proof shows by contradiction that the algorithm achieves the security goals under the intractability assumptions

The Diffie-Hellman protocol [DH76]

- 2-party key exchange protocol

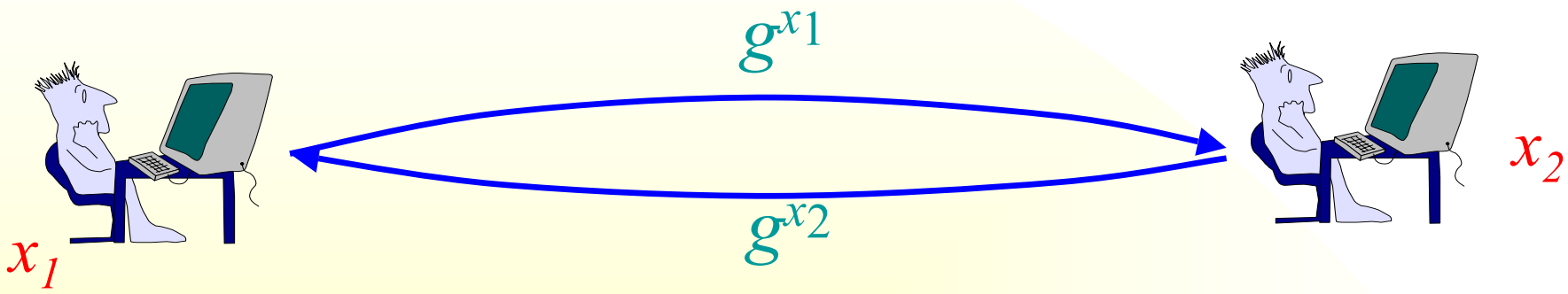


- Establishing a secure channel between two parties is reduced to the problem of generating a session key sk
- The session key is used to achieve data secrecy and integrity

The Diffie-Hellman problems

- Computational problem (CDH)
  - Given $g^{x}1$, $g^{x}2$, is the ennemy able to compute the shared secret $g^{x}1^{x}2$?
- Decisional problem (DDH)
  - Given $g^{x}1$, $g^{x}2$, is the ennemy able to distinguish the shared secret $g^{x}1^{x}2$ from a given random value g^{r} ?

Security of the DH protocol



- CDH assumption (weaker than DDH)
  - If CDH holds, the key $H(g^{x1x2})$ is semantically secure, in the random oracle model
- DDH assumption
  - If DDH holds, the key g^{x1x2} is semantically secure

Basic reductions to the discrete logarithm problem

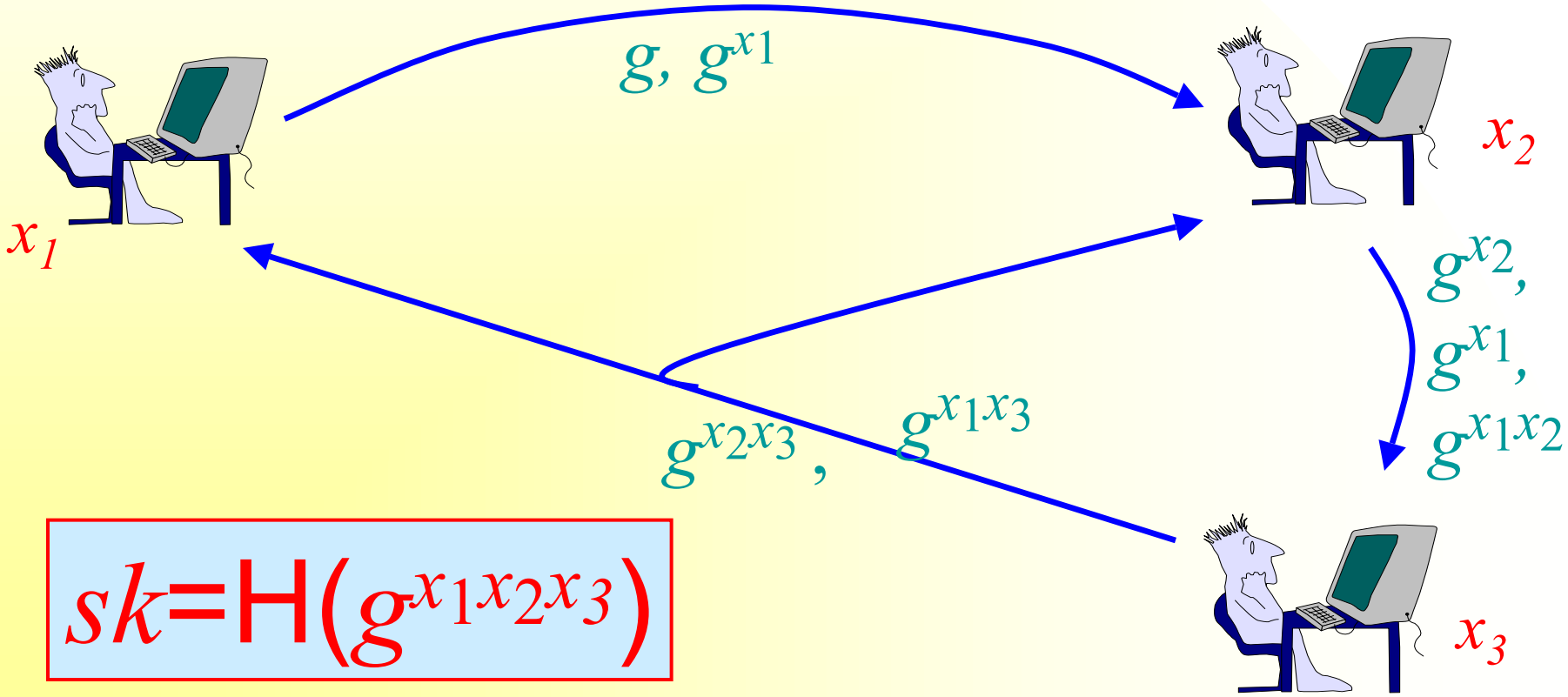
- Fix a multiplicative group G, and an element g
- Discrete logarithm problem (DL)
  - Given $y \in \langle g \rangle$, find x such that $y = g^x$
- One easily gets
  - DL => CDH => DDH

Group Diffie-Hellman Protocols

- Defined by three algorithms
  - *SETUP* *(all cases)*
  - *REMOVE* *(dynamic case)*
  - *JOIN* *(dynamic case)*
- The session key is
  - $sk = \mathrm{H}(g^{x_1 x_2 \ldots x_n})$

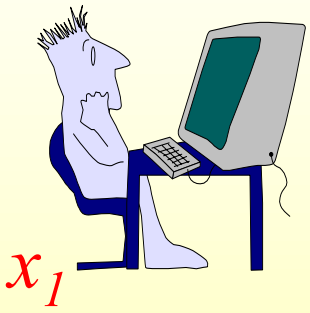
The *SETUP* Algorithm

- Ring-based protocols
- Compute step by step a generalized DH values



$$sk = \mathrm{H}(g^{x_1 x_2 x_3})$$

The *REMOVE* Algorithm

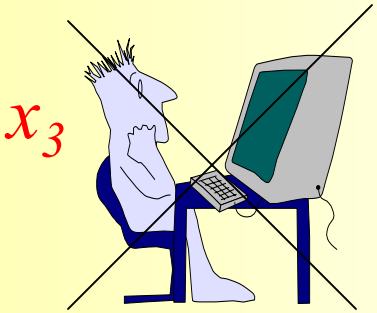


x_1

$g^{x'_2 x_3}$

x'_2

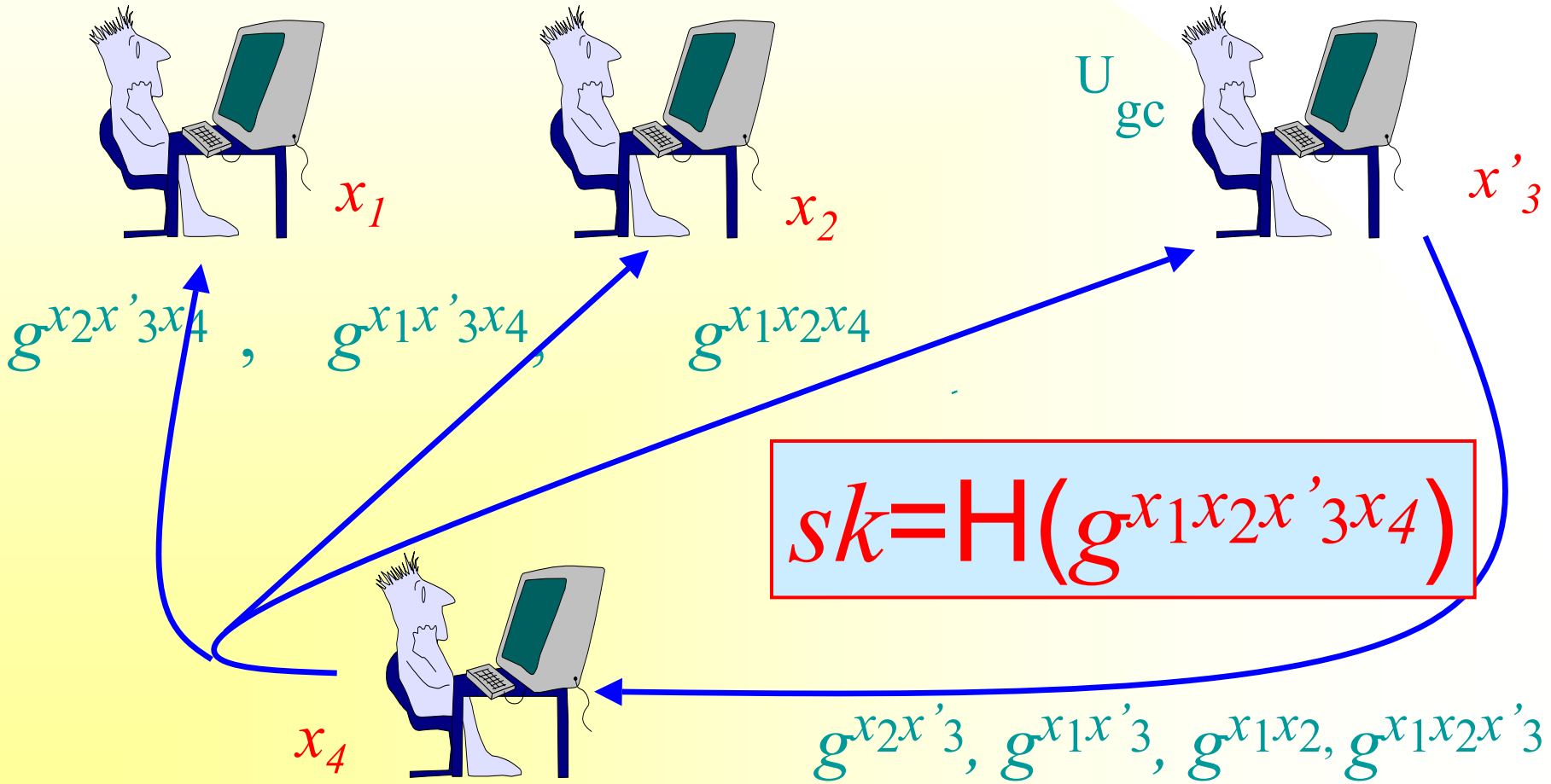
$$sk = H(g^{x_1 x'_2 x_3})$$



x_3

The *JOIN* Algorithm

- Initiated by player with the highest index in group



The Group Computational DH Assumption

- The CDH generalized to the multi-party case
  - given *some* subsets of indices in $I=\{1,\ldots,n\}$ and all the values $g^{\Pi_{i\in J} x_i}$ for every given subset J of I,
  - one has to compute the value $g^{x_1 \cdots x_n}$
- Example with four parties ($n=4$ and $I=\{1,2,3,4\}$)
  - given the values

$$g \quad , g^{x_1} \quad , g^{x_2} \quad , g^{x_1 x_2} \quad , g^{x_1} \quad , g^{x_2} \quad , g^{x_3} \quad , g^{x_1 x_2} \quad , g^{x_1 x_3} \quad , g^{x_2 x_3}$$

$$?? \quad , g^{x_1 x_2 x_3} \quad , g^{x_1 x_2 x_3} \quad , g^{x_1 x_2 x_4} \quad , g^{x_1 x_3 x_4} \quad , g^{x_2 x_3 x_4}$$

  - compute the last value $g^{x_1 x_2 x_3 x_4}$

The Group Decisional DH Assumption

- The DDH generalized to the multi-party case
  - given *some* subsets of indices in $I=\{1,\ldots,n\}$ and all the values $g^{\Pi_{i\in J} x_i}$ for every given subset J of I,
  - one has to distinguish the value $g^{x_1 \cdots x_n}$ from a random one
- Example with four parties ($n=4$ and $I=\{1,2,3,4\}$)
  - given the values

$$g,\ g^{x_1},\ g^{x_2},\ g^{x_1},\ g^{x_1 x_2},\ g^{x_1},\ g^{x_1 x_2},\ g^{x_1 x_2 x_3},\ g^{x_1},\ g^{x_1 x_3},\ g^{x_2 x_3},\ g^{x_1 x_2},\ g^{x_1 x_2 x_3},\ g^{x_1 x_2 x_4},\ g^{x_1 x_3 x_4},\ g^{x_2 x_3 x_4}$$

  - distinguish the last value $g^{x_1 x_2 x_3 x_4}$ from a random one

??

Reducing GDDH to DDH

- Let Γ_n be a collection of subsets of I_n={1,…,n}
  - E.g., the above triangular structure (flows)

- For a « good » type of collection of subsets,
  - $\mathrm{adv}^{\mathrm{gddh}_\Gamma}(t) \leq (2n-3)\mathrm{adv}^{\mathrm{ddh}}(t')$
  - with $t' \leq t+t_G\Sigma\gamma_i$ and where γ_i is the size of Γ_i

- We can see GDDH as a standard assumption !

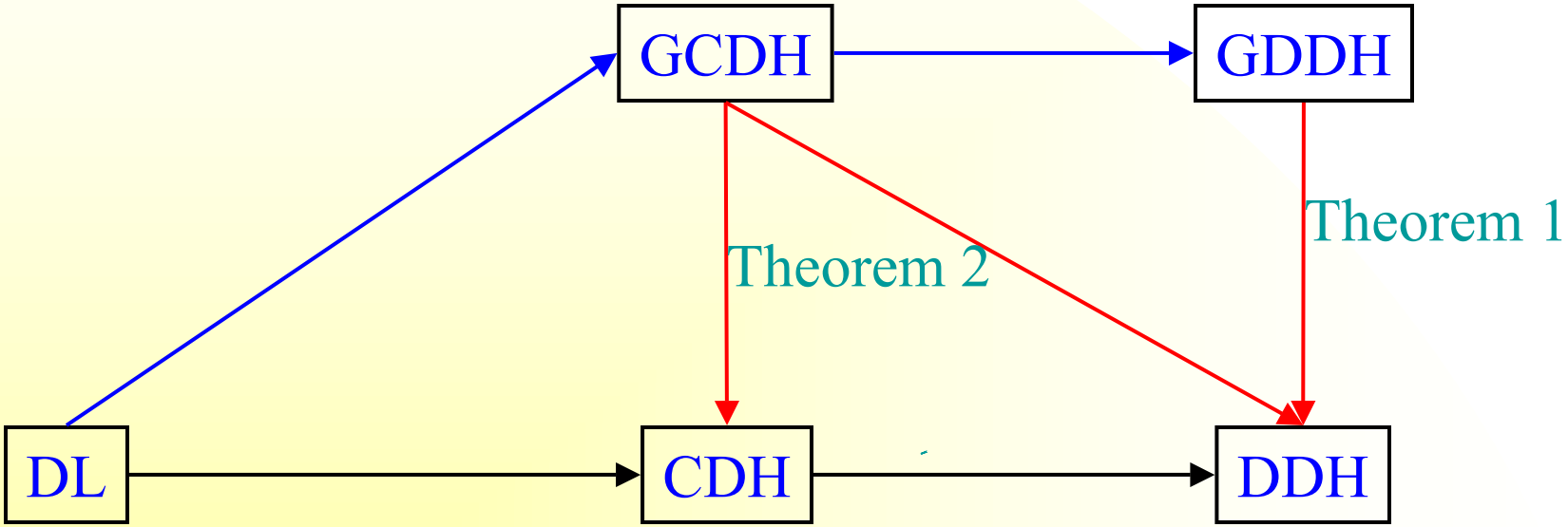
Reducing GCDH to DDH and CDH

- Let Γ_n be a collection of subsets of I_n={1,…,n}
  - E.g., the above triangular structure (flows)

- For a « good » type of collection of subsets,
  - $suc^{gcdh\Gamma}(t) \leq suc^{cdh}(t) + (n-2)adv^{ddh}(t')$
  - with $t' \leq t+t_G\Sigma\gamma_i$ and where γ_i is the size of Γ_i

- Can we see GCDH as a (hybrid) standard assumption ?

Hierarchy among problems



Conclusion and Future Work

- Contributions
  - Formalizing the group Diffie-Hellman problems
  - Studying the case where a reduction applies
  - Reducing GDH assumptions to DDH or, better, CDH
- Furture work
  - Reducing GCDH to CDH only ?